REMARKS

This amendment is in response to the Official Action dated November 28, 2007. Claims 1, 2, 3, 4, 9, 14, and 18 have been amended, claim 11 have been canceled; as such claims 1-4, 9, 11-24 are now pending in this application. Claims 1-4, 9, 14, 18, 20, and 22 are independent claims. Reconsideration and allowance is requested in view of the claim amendments and the following remarks.

No new matter has been added by this Amendment. Support for the amended claims can be found in the specification as filed. For example, support for the feature is described in connection with "a viewing apparatus ... for communicating with said image pickup device," is found in FIGS. 3, 5, and 10, showing that once authentication has taken place, communication between the image pickup device and the image viewer apparatus can occur directly.

Rejections under 35 U.S.C. § 101

Claim 18 have been amended is accordance with the suggestion set forth in the Final Office Action to overcome issues relating to statutory subject matter

An Example Embodiment

FIG. 1 illustrates an example embodiment of the present invention illustrating an image pickup device 100 attached to a network 600 via key generator 200. A viewer 400 can communicate directly with image pickup device 100, after authentication by authentication server 500. A viewer 400 seeking to communicate with image pickup device 100 will contact authentication server 500 with security information, such as a serial number for the image pickup device. The authentication server will conform that viewer 400 is qualified to communicate with image pickup device 100. Once authenticated, the viewer 400 can communicate directly with image pickup device. Since communication from the image pickup is encrypted, the viewer uses a removable storage device containing a decryption key to communicate with the image pickup device 100.

Rejections under 35 U.S.C. § 102

Claims 9, 11, 12, 14, 15, and 17 are rejected under 35 USC § 102 as anticipated by U.S. Patent Pub. No. 2002/0118837 to Hamilton.

> Claim 9 recites: *An image pickup apparatus unit comprising:*
>
> *an image pickup apparatus having a unique identifying number and having an encrypting function for encrypting a picked-up image for transmission to a network; and*
>
> *a removable recording medium for recording a decryption key for decrypting the image encrypted by said image pickup apparatus and the identifying number of said image pickup apparatus in association with each other.*
>
> *wherein said image pickup apparatus receives an encryption key for encrypting said image from a key generating apparatus;*
>
> *wherein said removable recording medium receives the decryption key for decrypting said image from a key generating apparatus.*

With respect to claim 9, Hamilton fails to teach or suggest *"a removable recording medium for recording a decryption key for decrypting the image encrypted by set image pickup apparatus and a identify number of set image pickup apparatus in association with each other...wherein said removable recording medium receives the decryption key for decrypting said image from a key generating apparatus."*

Hamilton is directed to systems where the authentication of an image is critical, e.g., in cases of insurance investigations and court photographs. The problems being remedied is that digital images are easily modified therefore a method for ensuring the authenticity of a given digital image may be critical for in such cases. To resolve these issues Hamilton makes sure an image is authentic by having each camera encrypt a given image and **not releasing the decryption mechanism to any entity outside of the authentication center.** However, encryption keys and serial numbers are used by outside of the authentication center to initialize a given camera.

When an image needs to be authenticated process illustrated in figure 5 is performed. Figure 5 illustrates that **instead of providing a decrypted image upon request the authentication**

center instead compares an image sent in with the authenticated image already stored in the database and provides a comparison of the results by doing a bit by bit comparison. The image stored at the authentication center is not viewed per se, but instead used to as a comparison against an image that is transmitted for authentication to the authentication center to ensure that the image sent in later is identical to the authenticated image already in the database.

In Hamilton the decryption key is never stored in the removable recording medium. More importantly, in Hamilton the decryption key is never released to any entity outside of the authentication center. By distinction claim 9 recites that the " *removable recording medium for recording a decryption key for decrypting the image encrypted by set image pickup apparatus and a identify number of set image pickup apparatus in association with each other...wherein said removable recording medium receives the decryption key for decrypting said image from a key generating apparatus.* "

Since Hamilton never allows the decryption key outside the authentication center, then the decryption key is not stored in a removable medium.

The portion of Hamilton cited by the Office Action simply cites to a mechanism for transferring an encryption key and serial number, **not a decryption key**.

Claim 14 recites "*said key generating apparatus generates the decryption key for decrypting said encrypted image by the viewing apparatus and transmits the decryption key to a removable recording medium for recording said decryption key and the identifying number of said image pickup-apparatus in association with each other.*"

Again, and as set forth above, Hamilton only discloses transmitting the encryption key to an optimization senator the actual encryption and decryption key is not stored or transmitted to the authorization center. Since Hamilton never allows the decryption key outside the authentication center, then the decryption key is not stored in a removable medium nor is the decryption key available to the viewer.

11

Application No. 10/809,532   Docket No.: SON-2960
Response to Office Action dated November 28, 2007
Amendment dated February 28, 2008

Hamilton therefore fails to teach or suggest various features of independent claims 9 and 14. Furthermore, at least for the reason disclosed above, claim 9 , and 15-17 overcome Hamilton because they depend on independent claims 9 and 14.

Accordingly, Applicant respectfully requests that the rejection of claims [] under 35 U.S.C. § 102(e) be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 1-4 have been rejection under 35 U.S.C. § 103 over U.S. Patent Pub. No. 2004/0066456 to Read in view of Hamilton. Claims 16 and 22-24 have been rejection under 35 U.S.C. § 103 over Hamilton in view of Read.

As Amended, claim 1 recites: *An image transmission system for transmitting an image via a network, said image transmission system comprising:*

> *one or a plurality of image pickup apparatus each having a unique identifying number and*
> > *having an encrypting function for encrypting a picked-up image for transmission to said*
> > *network;*
>
> *a key generating apparatus for generating, for each said image pickup apparatus, an*
> > *encryption key for encrypting said image and a decryption key for decrypting said*
> > *encrypted image;*
>
> *a removable recording medium for recording said decryption key and the identifying number*
> > *of said image pickup apparatus in association with each other;*
>
> *a viewing apparatus connected to said removable recording medium, having a decrypting*
> > *function for decrypting said encrypted image using said decryption key, for*
> > ***communicating with said image pickup device, and for viewing the image transmitted***
> > ***via said network from said image pickup apparatus to the viewing apparatus; and***
>
> *an authenticating server for authenticating said image pickup apparatus accessible from said*
> > *viewing apparatus.*

The amended claim language indicates that while authentication may take place at the authentication server, the image pickup device communicates the image to the viewing device over the network, without routing it through the authentication server.

With respect to claim 1, neither Read nor Hamilton disclose *"a viewing apparatus connected to said removable recording medium, having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to the viewing apparatus."*

Both Hamilton and Read force all communications between the user/viewer and any collected-images pass through the authentication server.

In Hamilton, all images are authenticated by the authentication server. These include any original images from the imaging device and any copies requiring authentication.

In Read, the disclosed central server retrieves and stores images from the imaging device 104 and 106, which can then be viewed by the End Users 110. There is no communication between the End User 110 and the Imaging devices directly.

By contrast, claim one recites that the" viewer apparatus…communicating with the image pickup device" and *"the image transmitted via said network **from said image pickup apparatus to the viewing apparatus.**"* Neither Hamilton nor Read, disclose this direct communication.

Even if Hamilton and Read were combinable (which is not admitted), Applicant submits that the combination would fail to teach or suggest *"viewer apparatus…communicating with the image pickup device"* and *"the image transmitted via said network **from said image pickup apparatus to the viewing apparatus.**"*. Instead, a combination of Hamilton and Read would necessarily yield a system to using an authentication server as a buffer between the viewer and imaging device even after authentication has taken place.

Since even a combination of the relied upon references would still fail to yield the claimed invention, Applicant submits that a prima facie case of obviousness for claim 1 has not been presented. For the reasons stated above claims 2-4, and 16, and 22-24 also overcome the Hamilton and Read.

13

Accordingly, Applicant respectfully requests that the rejection of independent claim 1-4 and under 35 U.S.C. § 103(a) be withdrawn.

Claims 18-21 have been rejection under 35 U.S.C. §103 over U.S. Patent Pub. No. 2004/0085446 to Park, in view of Read in view of U.S. Patent No. 6,999,588 to Oishi.

> Amended claim 18 recite: *A computer program, stored on a computer readable medium, for making a computer perform comprising the steps of:* ...
>> *requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup device;*
>> *authenticating the user and image pickup apparatus in response to the requesting step;*
>> *connecting the image pickup apparatus to a viewing apparatus;*
>> *comparing the identification number in the memory card to the identifying number of the image pickup apparatus;*
>> *obtaining the decryption key from the memory card;*
>> *transmitting an image request from the viewing apparatus to the image pickup apparatus;*
>> *receiving an image from the imaging pickup apparatus at the viewing apparatus;*
>> *decrypting images received from the image pickup device using the decryption key;*
>> *displaying the decrypted images on the viewer.*

With respect to claim 18, neither Park, Hamilton, nor Oishi teach or suggest the authentication steps of "*requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup device; authenticating the user and image pickup apparatus in response to the requesting step,*" and then the direct communication steps of "*transmitting an image request from the viewing apparatus to the image pickup apparatus.*"

Park describes a security system that allows remote monitoring of video cameras, but lacks the ability to use a common server to authenticate viewers.

Hamilton simply discloses a method of authenticating images at a central authentication server, which simply acts as an image repository for comparing an incoming image from a user with another image in the repository.

Finally, Oishi teaches a method by which images can be encrypted using an IC card.

However, all these references fail to teach or suggest the concept of initially passing communications through an authentication server to verify a viewer before allowing communication directly between the viewer and the imaging apparatus. That is none of the references allow both the use of an authentication server to begin communication and direct communication between the imaging device and the viewer thereafter. There is simply no motivation is any of the references to this twp part communication scheme.

Even if Park, Read, and Oishi were combinable (which is not admitted), Applicant submits that the combination would fail to teach or suggest *"authenticating the user and image pickup apparatus in response to the requesting step; connecting the image pickup apparatus to a viewing apparatus,"* and *"transmitting an image request from the viewing apparatus to the image pickup apparatus; receiving an image from the imaging pickup apparatus at the viewing apparatus."*

Instead, a combination of Park, Read, and Oishi would necessarily yield a video camera system as in Park, but which passes all communication through a central server like in Read, which uses the authentication mechanism in Oishi.

Since even a combination of the relied upon references would still fail to yield the claimed invention, Applicant submits that a prima facie case of obviousness for claim 18 has not been presented. Applicant also notes that the offered combination appears to be a (failed) attempt to reconstruct the claimed invention in hindsight, as there is no basis to combine Park, Read, and Oishi to produce the claimed invention..

For similar reasons claim 20 also overcomes the combination of Park, Read, and Oishi. For the reasons stated above claims 19 and 21 also overcome the combination of Park, Read, and Oishi because they depend on independent claim 18 and 20.

Accordingly, Applicant respectfully requests that the rejection of independent claim 18 and dependent claims 19-21 under 35 U.S.C. § 103(a) be withdrawn.
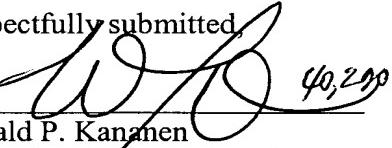
In view of the above amendment, applicant believes the pending application is in condition

for allowance.

CONCLUSION

Applicant believes no fee is due with this response. However, if a fee is due, please

charge our Deposit Account No. 18-0013, under Order No. SON-2960 from which the undersigned

is authorized to draw.

Dated: February 28, 2008   Respectfully submitted,

By_____
Ronald P. Kananen
    Registration No.: 24,104
Christopher M. Tobin
    Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
Attorneys for Applicant